

FDA Issues Reminder on Cybersecurity for Networked Medical Devices

The U.S. Food and Drug Administration (FDA) has issued a “reminder” notice entitled “Cybersecurity for Networked Medical Devices is a Shared Responsibility.” It is intended for medical device manufacturers, hospitals, device user facilities and users, healthcare IT and procurement staff, and biomedical engineers.

“The notice was issued because many in the target audience don’t know this guidance exists,” says John Murray, software compliance expert for the FDA. “We’ve seen confusion in the community.”

Although the notice does not contain new information, Murray says it reminds interested parties of the existing guidance document as an important resource. He says the notice has three main messages:

- Cybersecurity for medical devices is a shared risk, shared responsibility environment.
- Typically, FDA approval is not necessary for cybersecurity upgrades.
- There is a guidance document available from FDA that offers detailed information on this topic.

The following information is reprinted from that notice.

Issue

FDA wants to remind you that cybersecurity for medical devices and their associated communication networks is a shared responsibility between medical device manufacturers and medical device user facilities. The proper maintenance of cybersecurity for medical devices and hospital networks is vitally important to public health because it ensures the integrity of the computer networks that support medical devices.

FDA is aware of misinterpretation of the regulations for the cybersecurity of medical devices that are connected to computer networks. FDA’s interpretation of the regulations can be found in the 2005 guidance for industry and its accompanying information for healthcare organizations.

FDA wants to emphasize the following:

- Medical device manufacturers and user facilities should work together to ensure that cybersecurity threats are addressed in a timely manner.
- The agency typically does not need to review or approve medical device software changes made for cybersecurity reasons.
- All software changes that address cybersecurity threats should be validated before installation to ensure they do not affect the safety and effectiveness of the medical devices.

Software patches and updates are essential to the continued safe and effective performance of medical devices. Typically, FDA approval is not required before installing changes, updates, or patches that address cybersecurity issues (see question #10 of the guidance). Software patches usually do not involve FDA review because most patches are installed to reduce the risk of a cybersecurity problem and not to address a risk to health posed by the device.

The need to be alert and responsive to cybersecurity issues is part of the device manufacturer’s obligation. FDA recommends that purchasers and users of medical devices that may have a cybersecurity problem contact the device manufacturer with their concerns.

Take Action

There are some simple ways to help to protect against cybersecurity threats like viruses and worms that affect medical devices:

- Prior to installing any computerized equipment involving medical devices, make sure that the equipment is virus free.
- Make sure that you have adequate anti-virus software and firewalls installed, properly set up and current.
- Update your operating system and medical device software. Software updates offer the latest protection against harmful activities.
- Validate all changes, updates, and patches, including operating systems, before installing them to ensure the safety and effectiveness of the medical devices.
- Purchasers and users of medical devices that may have a cybersecurity problem should contact the device manufacturer with their concerns. ■

Cybersecurity Resources

1. Guidance for Industry—Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (issued January 2005). Available at <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm>.
2. Information for Healthcare Organizations about FDA’s “Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software.” Available at <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm070634.htm>.
3. National Cybersecurity Awareness Month Website. Available at http://www.dhs.gov/files/programs/gc_1158611596104.shtm.
4. FDA’s MedSun Medical Product Safety Network: “Cybersecurity of Medical Devices.” Available at <http://www.fda.gov/MedicalDevices/Safety/MedSunMedicalProductSafetyNetwork/ucm127816.htm>.